SECURITY AND PRIVACY IN BIOMETRICS – A REVIEW

Sanjay Ganesh Kanade[1], Ashish P. Kinge[2], Dhananjay S. Sargar[3], Kirti S. Kanade[4]
[1, 2, 3]Department of Electrical Engg., TSSM's Bhivarabai Sawant College of Engineering and Research, Narhe, Pune
[4]BAG Electronics Pvt. Ltd., Pune

Abstract
Biometrics, which provides strong user authentication, comes with some severe drawbacks of lack of privacy protection. Therefore, various methods have been proposed in literature which add privacy and improve security of biometric systems. A thorough review of these crypto-biometric systems is presented in this paper. The crypto-biometric systems are systematically classified into various categories on the basis of their fundamental way of working. Additionally, guidelines are also provided for performance evaluation comparison between various crypto-biometric systems which could be using any underlying biometric modality.

Index Terms: Biometrics, Security and Privacy, Template Protection

I. INTRODUCTION

Biometrics is defined as automated recognition of individuals based on their behavioral and biological characteristics [1]. Figure 1 shows a block diagram of a generic biometric system. Biometric recognition provides a strong link between the user's identity and the authenticator. However, since, the biometric data are permanently associated with the user, they cannot be replaced in case of a compromise. Moreover, there are privacy risks associated with the use of biometrics. The biometric data stored in various databases can be interlinked to steal the private information of the user.

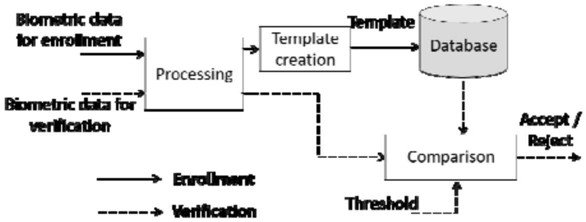


Figure 1 Diagram depicting a generic biometric system

Fortunately, there are ways to tackle this problem by combining biometrics with cryptographic techniques. Cryptography deals with protecting information while it is being stored or transmitted by means of some user defined secrets like passwords. Figure 2 shows a generic cryptographic system. These two techniques have complementary characteristics and can be combined to design better and more secure systems. The strong association of biometric characteristics with the user's identity can be utilized to provide the trust required in cryptography. Moreover, the cryptographic techniques can be employed to provide protection to the biometric data without compromising privacy.

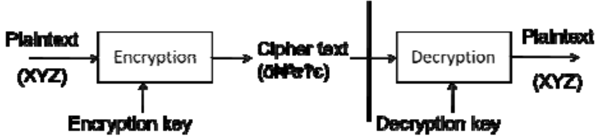


Figure 2 A generic cryptographic system

II. NEED OF INCORPORATING SECURITY AND PRIVACY IN BIOMETRIC SYSTEMS

In spite of providing the advantage of a strong link between a person and his identity, biometric systems suffer from some drawbacks [2]. These drawbacks are described in the next subsection.

II.A Problems Associated with Biometrics

There are two important issues related to biometric systems:

- **Non-revocability:** The biometric data of a person cannot be canceled or replaced. Therefore, in case of a compromise, the person cannot use the same biometric characteristic in that system and possibly in all other systems based on the same biometric characteristic. This is called non-revocability or non-cancelability of biometrics.
- **Privacy compromise:** Protecting the privacy of a user is becoming prominent with an increasing use of biometric systems. Three types of privacy compromises have been defined in [kanade-thesis, kanade-book]:
    - *Biometric data privacy compromise:* The raw biometric data of the user can be recovered from the stored templates. The synthesized data can be provided to the system to gain access and can also reveal some physical conditions.
    - *Information privacy compromise:* Cross database matching between two biometric based systems is possible, and thus, the information stored in that system can be compromised.
    - *Identity privacy compromise:* A person can be tracked from one system to another by cross-matching his templates from the two biometric databases. This can be considered as a compromise of user's privacy.

These drawbacks of biometrics systems have motivated the research in the field of privacy preserving biometric systems.

III. GENERAL CLASSIFICATION OF PRIVACY PRESERVING CRYPTO-BIOMETRIC SYSTEMS

In this section, a general classification of privacy preserving crypto-biometric systems is presented. This classification is depicted in Fig. 3 [2, 3].

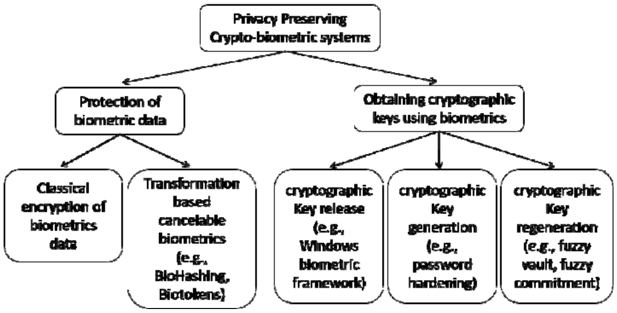

Privacy Preserving Crypto-biometric systems
Protection of biometric data
Obtaining cryptographic keys using biometrics
Classical encryption of biometrics data
Transformation based cancelable biometrics (e.g., BioHashing, Biotokens)
cryptographic Key release (e.g., Windows biometric framework)
cryptographic Key generation (e.g., password hardening)
cryptographic Key regeneration (e.g., fuzzy vault, fuzzy commitment)

Figure 3 Systematic classification of crypto-biometric systems

As described earlier, biometrics and cryptography have certain limitations. Crypto-biometric systems attempt to eliminate these limitations by combining the two techniques. Based on their application and functionality, these systems are classified into two main categories as: (a) Protection of biometric data, and (b) Obtaining cryptographic keys with biometrics [2].

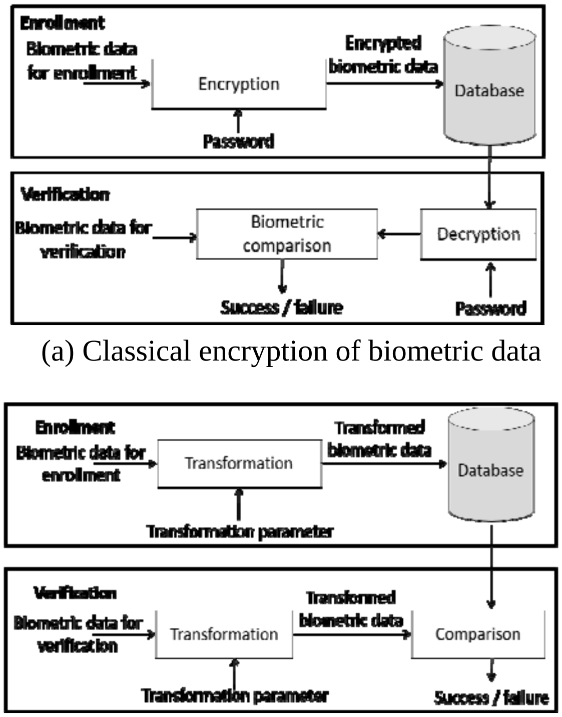
In the first category, cryptographic techniques, such as encryption, hashing, transformation, etc., are used to protect the biometric data. The outcome of these systems is a one-bit verification result similar to the classical biometric systems. On the other hand, in the systems from the second category, biometric data is used to obtain cryptographic keys (denoted as crypto-bio keys). The systems in these two categories are further divided depending on how these techniques are combined.

III.A PROTECTION OF BIOMETRIC DATA

The systems in this category use cryptographic techniques to add some of the desired characteristics (such as revocability, privacy protection, etc.) to biometrics based verification systems.

These systems are divided in two subcategories as: (1) systems using classical encryption of biometric data, (2) systems employing transformation based cancellable biometrics [4, 5, 6, 7, 8]. The first solution is a simplest one where the biometric template is encrypted with a user specific password before storing in a database. Before comparison, the biometric data is decrypted. The systems in second subcategory differ from this in a significant way where the comparison is carried out in the transformed domain itself. The transformation applied to the biometric data in this case is user specific based on a personal secret. In this way, revocability is added into the biometric system. However, the systems in the category ‘Protection of biometric data’ can only be used for user authentication and not for cryptographic purposes.

Figure 4 shows generic structures of systems in these two subcategories.



(a) Classical encryption of biometric data

(b) Transformation based cancellable biometrics

Figure 4 Systems providing protection to the biometric data

III.B OBTAINING CRYPTOGRAPHIC KEYS USING BIOMETRICS

The second major category in crypto-biometric systems is where cryptographically usable keys are obtained with the help of biometrics. These systems are sub-classified in three categories: (a) key release, (b) key generation, and (c) key regeneration.

III.B.1 Biometrics based Cryptographic Key Release Systems

The easiest way to integrate biometric systems in a cryptographic framework is to store cryptographic keys securely and release them only after successful biometric verification. This type of mechanism is already implemented in PCs and smartphones. However, the drawback of such systems is that the biometric comparison is carried out in the classical way, and therefore, inherits most of the drawbacks of the classical biometrics based systems.

III.B.2 Biometrics based Cryptographic Key Generation

From security point of view, a better solution than the key release is to generate a stable bit-string directly from the biometrics. These systems do not need to store the biometric template but they only store a verification string which is generally a hashed version of the biometrically generated key. At the time of verification, an attempt is made to obtain the cryptographic key which in genuine case should match the key generated at the time of enrollment. The verification decision is taken based on the comparison between the verification string only.

In this way, the system avoids storage of biometric data (template) thereby removing some of the advantages of the classical biometric system.

III.B.3 Biometrics based Cryptographic Key Regeneration

The third sub-category, biometrics based cryptographic key regeneration, is the most appealing type of systems in which a randomly generated key is intrinsically bound to the biometric data at the time of enrollment [9, 10, 11, 12, 13, 14]. The same key is regenerated at the time of verification by supplying another biometric data of the same user.

In this type of systems, the stored data does not leak any information about the user identity. Thus, it provides complete security and privacy while providing biometrics based strong user authentication. The outcome of the system is a long cryptographically secure key which can be directly used for cryptographic applications such as encryption.

All these three subcategories for obtaining cryptographic keys using biometrics are shown in generic form in Fig. 5.

IV. GENERAL GUIDELINES FOR PERFORMANCE EVALUATION AND COMPARISON OF CRYPTO-BIOMETRIC SYSTEMS

The crypto-biometric systems when presented for performance comparison are found to be based on different biometric modalities. Therefore, the performance comparison in terms of absolute values of False Acceptance Rate

(FAR), False Rejection Rate (FRR), and /or Equal Error Rate (EER) is irrelevant. Therefore, it is customary to compare the performance of the crypto-biometric system with the baseline biometric system it uses. In this way, one can get a fair idea of the effects of the modifications on the performance. Moreover, since the crypto-biometric systems involve some secret parameter (a key, or a password) along with biometric data, it is required to know the effect of compromise of one of the factors on the overall system performance.

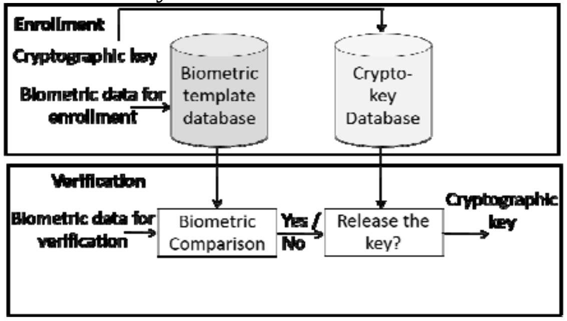
In view of this, it is suggested that the experimental performance evaluation of these kind of systems should be carried out in following scenarios:

i. **Ideal case:** No data is compromised,

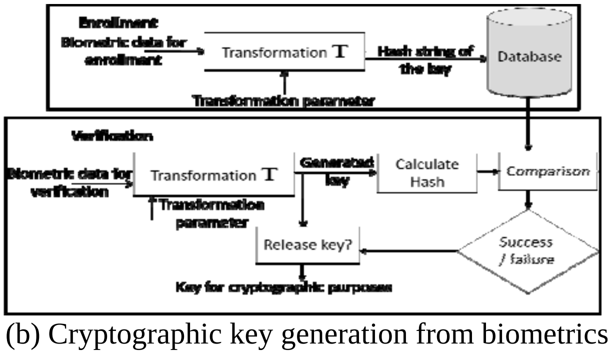
ii.**Stolen key:** the key or transformation parameter used along with biometrics is compromised. In this case, the resilience of the system is tested,

iii. **Stolen biometric:** the biometric data of the user is stolen. This illustrates the security protection added by the transformation parameter.

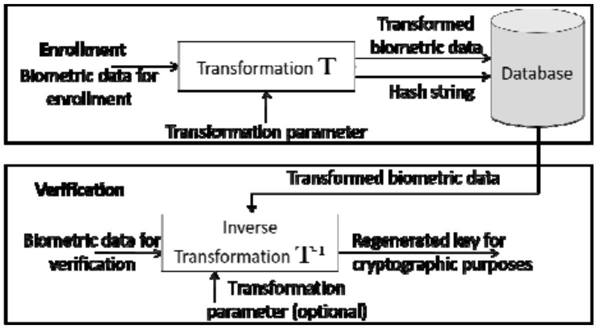
These systems are supposed to provide security and privacy in the biometrics based authentication systems. Therefore, theoretical security analysis of these systems should also be carried out. This analysis would reveal the strength of the cryptographic keys generated with these systems in attach scenarios.



(a) Cryptographic key release based on biometrics



(b) Cryptographic key generation from biometrics


Enrollment
Biometric data for enrollment
Transformation T
Transformed biometric data
Database
Hash string
Transformation parameter
Verification
Transformed biometric data
Biometric data for verification
Inverse Transformation T-1
Regenerated key for cryptographic purposes
Transformation parameter (optional)

(c) Cryptographic key regeneration using biometrics

Figure 5 Systems which attempt to obtain cryptographic keys with the help of biometrics

V. CONCLUSIONS

In this paper a thorough review of the crypto-biometric systems is presented in a systematic way along with their classification. Crypto-biometric systems add privacy and security to biometrics based authentication systems thereby enhancing their reliability and increasing their acceptance among wider public, especially those against biometrics because of privacy threats. Guidelines for experimental performance evaluation as well as comparison between the crypto-biometric systems are also given which could be useful to the researchers to carry out further research in this field.

REFERENCES

[1] ISO/IEC CD 2382.37. Information processing systems Vocabulary Part 37 : Harmonized Biometric Vocabulary, 2010

[2] Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. “Enhancing Information Security and Privacy by Combining Biometrics with Cryptography”, Synthesis lectures on Security, Privacy and Trust, Morgan and Claypool publishers, available (online and print) June 2012, 140 pages.

[3] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008 (Article ID 579416):17 pages

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614–634, 2001

[5] Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. “Cancelable Biometrics for Better Security and Privacy in Biometric Systems”, Advances in Computing and Communications, volume 192 of Communications in Computer and Information Science, pages 20-34, Springer Berlin Heidelberg, 2011

[6] Andrew Teoh Beng Jin, David Ngo, Chek Ling, and Alwyn Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition, 37(11):2245–2255, November 2004

[7] Alessandra Lumini and Loris Nanni. An improved biohashing for human authentication. Pattern Recognition, 40(3):1057–1065, March 2007

[8] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In IEEE Conference on Computer Vision and Pattern Recognition, pages 1–8, June 2007

[9] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS), pages 28–36, 1999

[10] A. Juels and M. Sudan. A fuzzy vault scheme. In A. Lapidoth and E. Teletar, editors, Proc. IEEE Int. Symp. Information Theory, page 408. IEEE Press, 2002

[11] Feng Hao, Ross Anderson, and John Daugman. Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9):1081–1088, 2006

[12] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Z´emor. Optimal Iris Fuzzy Sketches. In IEEE Conference on Biometrics: Theory, Applications and Systems, 2007

[13] Sanjay G. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi. “Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris”. In The 6th Biometrics Symposium 2008 (BSYM2008), Tampa, FL, USA, September 2008

[14] Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. “Multi-biometrics Based Crypto-biometric Session Key Generation and Sharing Protocol”, In ACM Workshop on Mumtimedia and Security (MM&Sec), Niagara Falls/Buffalo, NY, USA, September, 2011